

[Previous Doc](#)   [Next Doc](#)   [Go to Doc#](#)  
[First Hit](#)



Generate Collection

B

L2: Entry 17 of 17

File: JPAB

Feb 14, 2003

PUB-NO: JP02003044232A

DOCUMENT-IDENTIFIER: JP 2003044232 A 1

TITLE: DATA DISTRIBUTION METHOD, TERMINAL, SERVER, DATA DISTRIBUTION SYSTEM, ITS PROGRAM, AND RECORDING MEDIUM WITH THE PROGRAM RECORDED THEREON

PUBN-DATE: February 14, 2003

## INVENTOR-INFORMATION:

NAME

COUNTRY

SAWANO, TAKASHI

## ASSIGNEE-INFORMATION:

NAME

COUNTRY

SHARP CORP

APPL-NO: JP2001230488

APPL-DATE: July 30, 2001

INT-CL (IPC): G06F 3/12; G06F 17/60

## ABSTRACT:

PROBLEM TO BE SOLVED: To realize a data distribution system suitable for print data distribution, capable of preventing illegal use.

SOLUTION: A terminal 2 temporarily records encrypted print data in a print data reserving region. The terminal 2 recognizes the recorded print data, and communicates with a server 3 preliminarily decided for the decoding permission of the print data, and requests a password for authentication, and asks the server 3 to get the decoding permission of the print data. The terminal 2 decodes only the print data whose decoding is permitted from the server 3 whose authentication is successful, and allows a connected pointer to print the print data, and then erases the print data from the print data preserving region.

COPYRIGHT: (C)2003, JPO

[Previous Doc](#)   [Next Doc](#)   [Go to Doc#](#)

Terminal 2  
preserve region  
Server 3  
password request  
password

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-44232

(P2003-44232A)

(43) 公開日 平成15年2月14日 (2003.2.14)

(51) IntCl.<sup>7</sup>

G 0 6 F 3/12

識別記号

17/60

1 4 2

3 0 2

3 3 2

F I

G 0 6 F 3/12

17/60

テーマコード(参考)

A 5 B 0 2 1

K

1 4 2

3 0 2 E

3 3 2

審査請求 未請求 請求項の数18 OL (全 21 頁)

(21) 出願番号 特願2001-230488(P2001-230488)

(22) 出願日 平成13年7月30日 (2001.7.30)

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 澤野 貴

大阪府大阪市阿倍野区長池町22番22号 シ

ャープ株式会社内

(74) 代理人 100080034

弁理士 原 謙三

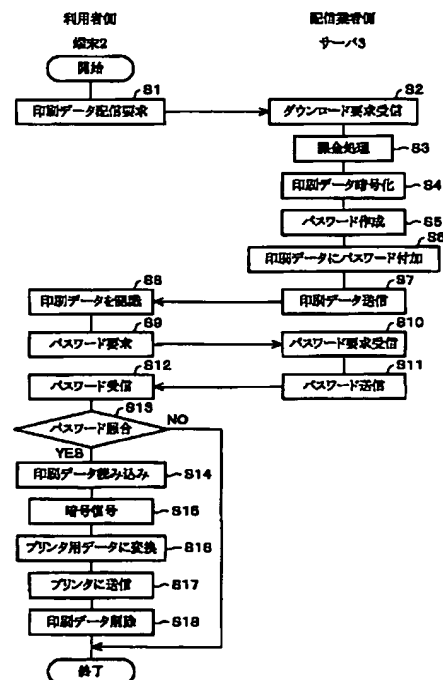
Fターム(参考) 5B021 AA01 BB02 LL01

(54) 【発明の名称】 データ配信方法、端末、サーバ、データ配信システム、並びに、そのプログラム、および、それが記録された記録媒体

(57) 【要約】

【課題】 不正利用を防止することのできる、印刷データ配信に適した、データ配信システムを実現する。

【解決手段】 端末2は、暗号化された印刷データを印刷データ保存領域に一時的に記録する。端末2が、記録された印刷データを認識し、印刷データの復号許可用に予め定められたサーバ3と通信して、認証のためのパスワードを要求するとともに、印刷データの復号許可を上記サーバ3に求める。端末2が、認証に成功した上記サーバ3から復号を許可された印刷データのみを、復号して、接続されたプリンタに印刷させ、印刷させた後に印刷データを上記印刷データ保存領域から消去する。



## 【特許請求の範囲】

【請求項1】端末に接続された出力手段によって製作物を製作するための暗号化された配信データを、サーバから上記端末に配信し、当該端末の記録手段に格納する配信工程と、

上記端末が、上記サーバと通信して出力許可を受け取った場合にのみ暗号化された配信データを復号する復号工程と、

上記端末が、復号された配信データに基づいて、上記出力手段に製作物を出力させる出力工程と、

上記出力工程の後、上記記録手段から配信データを消去する消去工程とを含んでいることを特徴とするデータ配信方法。

【請求項2】上記配信データは、上記出力手段としてのプリンタに、上記製作物としてのプリント物を出力させるためのデータであることを特徴とする請求項1記載のデータ配信方法。

【請求項3】上記復号工程は、出力許可を受けるサーバを認証する工程を含み、正規のサーバから出力許可を受け取った場合にのみ復号することを特徴とする請求項1または2記載のデータ配信方法。

【請求項4】さらに上記サーバが、上記端末にパスワードを送信する工程と、

上記端末が、上記パスワードに応じて上記サーバにパスワード要求を送信する工程と、

上記サーバが、送信したパスワードと受信したパスワード要求とを比較して正規の端末であるか否かについて上記端末を認証する工程とを含み、

認証に失敗した場合には、上記出力許可を上記端末に送信しないことを特徴とする請求項1、2または3のいずれかに記載のデータ配信方法。

【請求項5】さらに、上記配信工程の前に、上記配信データの配信される端末が上記消去工程を行う端末か否かを、上記サーバが確認する確認工程を含み、上記サーバは、確認できた場合にのみ、配信データを配信することを特徴とする請求項1、2、3または4のいずれかに記載のデータ配信方法。

【請求項6】さらに上記サーバが上記端末に第1のパスワードを送信し、上記端末が上記サーバに第1のパスワードに応じたパスワード要求を送信する、パスワード交換工程と、

上記サーバが、送信した第1のパスワードと受信したパスワード要求とを比較して正規の端末であるか否かについて上記端末を認証する、端末認証工程と、

認証が成功した場合に、上記サーバが、上記端末に上記出力許可として受信したパスワード要求に応じた第2のパスワードを送信する、再送信工程と、

上記端末が、送信したパスワード要求と受信した第2のパスワードとを比較して正規のサーバであるか否かについて上記サーバを認証する、サーバ認証工程とを含むこ

とを特徴とする請求項1または2記載のデータ配信方法。

【請求項7】出力手段によって製作物を製作するための暗号化された配信データを記録する記録手段と、

配信データの配信をサーバに要求し、上記記録手段に格納する配信要求手段と、

上記サーバと通信して出力許可を受け取った場合にのみ記録手段に格納された配信データを復号する復号手段と、

10 復号された配信データに応じた製作物を、上記出力手段に出力させる出力指示手段と、

上記出力手段が製作物を出力した後、上記記録手段から配信データを消去する消去手段とを備えていることを特徴とする端末。

【請求項8】端末に接続された出力手段によって製作物を製作するための配信データを格納する配信データ保存手段と、

暗号化された配信データの出力許可を上記端末へ送信する出力許可手段と、

20 上記出力許可に応じて上記出力手段が製造物を出力した後で自らの配信データを消去する消去手段が設けられている端末から、配信要求を受けた場合、当該端末に暗号化した配信データを送信する配信手段とを備えていることを特徴とするサーバ。

【請求項9】さらに、上記端末にパスワードを送信し、その後に上記端末が上記パスワードに応じて上記サーバに送信するパスワード要求を受信し、それとともに、送信したパスワードと受信したパスワード要求とを比較して正規の端末であるか否かについて上記端末を認証し、  
30 認証に失敗した場合には上記出力許可を上記端末へ送信しない認証手段を備えていることを特徴とする請求項8記載のサーバ。

【請求項10】上記端末から配信要求を受けた場合に、当該端末が、上記消去手段を備えているか否かを確認し、確認できた場合にのみ、上記配信手段に配信させる確認手段が設けられていることを特徴とする請求項8または9記載のサーバ。

【請求項11】上記確認手段によって、上記端末が消去手段を備えていないと判断された場合、上記端末を上記消去手段として動作させるためのプログラムまたはデータを、上記端末に送信する送信手段を備えていることを特徴とする請求項10記載のサーバ。

【請求項12】上記サーバには、上記配信手段が配信する配信データを、可変の暗号キーで暗号化する暗号化手段と、

上記配信手段が配信する配信データの復号キーを示すデータを配信先の上記端末へ通知する復号キー通知手段とが設けられていることを特徴とする請求項11記載のサーバ。

50 【請求項13】上記端末への配信データの配信に応じて

課金処理する課金手段を備えていることを特徴とする請求項8、9、10、11または12のいずれか記載のサーバ。

【請求項14】請求項7記載の端末と、上記端末に接続された出力手段によって製作物を製作するための配信データを格納する配信データ保存手段、上記出力許可を上記端末へ送信する出力許可手段、および、上記端末から配信要求を受けた場合、当該端末に暗号化した配信データを送信する配信手段が設けられているサーバとを含んでいることを特徴とするデータ配信システム。

【請求項15】記録手段を備えるコンピュータで実行するためのプログラムであって、サーバと通信して、出力手段によって製作物を製作するための配信データの出力許可を受け取った場合にのみ、上記記録手段に格納され、暗号化されている配信データを復号し、上記出力手段に出力させる出力指示手段、並びに、

上記出力手段が製作物を出力した後、上記記録手段から配信データを消去する消去手段として、上記コンピュータを実行させるプログラム。

【請求項16】請求項15記載のプログラムが記録された記録媒体。

【請求項17】請求項8、9、10、11、12または13のいずれか記載のサーバの各手段として、コンピュータを動作させるためのプログラム。

【請求項18】請求項17記載のプログラムが記録された記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークを介して、利用者の所望とするデータを配信するための、データ配信方法、端末、サーバ、データ配信システム、並びに、そのプログラム、および、それが記録された記録媒体に関するものである。

【0002】

【従来の技術】従来より、様々なコンテンツの、音楽、コンピュータソフト、ゲームソフトのデータが、ネットワークを介して配信されている。その配信の方法としては、例えば、オン・デマンド型と呼ばれる形式が知られている。この場合、利用者は、配信事業者のサーバコンピュータにアクセスし、そこに蓄積してあるコンテンツデータの中から、希望するものをダウンロードすることになる。このような配信方法においては、利用者は、希望するコンテンツデータを、欲しい時にすぐ手に入れることができる。

【0003】上記の形態において、利用者がデータ配信システムを利用するためには、例えば、あらかじめ配信事業者と契約を交わし、コンテンツを再生、記録するための専用の受信装置を備える必要がある場合がある。ま

た、他の例として、専用の通信プログラム等が記録されたCD-ROM等を購入して端末に搭載し、そして配信されたデータを記録再生するための装置を備える必要がある場合もある。そのように、配信されたデータが、利用者によって記録装置や記録媒体に記録され、繰り返し利用されるような場合においては、契約内容を逸脱した再生やコピー等を防止する必要がある。

【0004】そこで、コンテンツデータの記録保存を可能にしつつ、再生やコピー等の実行について契約内容を逸脱しないように、配信事業者側で規制できるようにするための技術が提案されている。

【0005】例えば、特開平10-207808号公報においては、コンテンツ配信の技術として以下に述べるような方法が提案されている。CD-Rにデバイスドライバ格納領域とデータ格納領域とを設け、デバイスドライバ領域には予め通信プログラム、暗号化のためのID、コピー禁止コード検出プログラム、CD-Rへの記録のためのプログラム、復号および再生に関するプログラムなどが記録され、またデータ格納領域にはネットワークを通じて配信されたコンテンツが記録される。このような構成にすることにより、上記のデータ配信に伴う使用権または著作権などの問題点を解決している。

【0006】

【発明が解決しようとする課題】しかしながら、印刷データ配信に、上述のデータ配信システムを用いると、音楽、コンピュータソフト、ゲームソフトのように、繰り返し使用されるコンテンツを配信することを前提としているため、印刷後は不要であるにもかかわらず、印刷データは、端末側で記録保存されることになる。したがって、印刷データを暗号化して配信したとしても、印刷データの複製物が端末に残り、端末の利用者が、当該印刷データの不正利用を試みる虞れがある。したがって、印刷データの著作権を十分に保護することが難しく、著作権者に配信許可を促すことが難しい。

【0007】また、上述のデータ配信システムにおいては、印刷後には不要な印刷データも、記録保存されてしまうので、端末の利用者が当該印刷データを削除する手間が必要となるという問題を生ずる。

【0008】このように、端末側で製作物を製作するためのデータを、端末に配信する場合に、上述のデータ配信システムを用いると、上記印刷データが記録保存されることにより、不正利用の虞れが生じ、また、削除の手間が必要となる問題が生ずる。

【0009】本発明は、上記の問題点を鑑みてなされたものであり、その目的は、利用者に手間をかけることなく、端末に必要な記録容量を削減できると共に、配信データの不正利用の防止能力の高い、データ配信方法、端末、サーバ、データ配信システム、並びに、そのプログラム、および、それが記録された記録媒体を実現することにある。

【0010】

【課題を解決するための手段】本発明に係るデータ配信方法は、上記課題を解決するために、以下の手段を講じたことを特徴としている。すなわち、端末に接続された出力手段によって製作物を製作するための暗号化された配信データを、サーバから上記端末に配信し、当該端末の記録手段に格納する配信工程と、上記端末が、上記サーバと通信して出力許可を受け取った場合にのみ暗号化された配信データを復号する復号工程と、上記端末が、

復号された配信データに基づいて、上記出力手段に製作物を出力させる出力工程と、上記出力工程の後、上記記録手段から配信データを消去する消去工程とを含んでいることを特徴としている。

【0011】このようなデータ配信方法の例としては、プリンタに接続された端末に印刷するためのデータを送信する場合、コンピュータ制御可能なミシンに刺繍パターンのデータを送信する場合、コンピュータ制御可能な工作機械に制御データを送信する場合、コンピュータ制御される電子レンジにレシピを送信する場合などがある。なお、上記の配信工程の後に、とぎれることなく行われる復号工程、出力工程、および、消去工程は、間に別の工程を含んでも構わない。

【0012】上記構成によれば、出力が終わるとともに、記録手段から配信データは削除されるので、出力後における、配信データの不正な複製および利用を防ぐことができる。

【0013】製作物が残るため不要となる配信データは、出力後には消去されるので、利用者にとって無駄な記録容量を使わずに済む。また、利用者自身による消去の作業は不要になるので、利用者にとって出力処理が簡単となる。

【0014】さらに、配信する際、配信データは暗号化されており、出力せずに中身を見ることはできず、また、復号せずに出力したとしても、意味のない製作物しか得ることができない。また、出力許可を受け取った場合にのみ復号、出力、消去をするので、その配信データを1度だけ出力することができる。したがって、端末側で複製することによる不正利用を防ぐことができる。

【0015】さらに、上記の方法においては、配信データは必ず出力を行なった後に消去されるので、間違えて出力前に配信データを消去するということは起こらない。また、配信データは出力後に消去されるので、配信データの複製物は端末に残らず、端末の利用者が当該配信データの不正利用を試みる虞れを防ぐことができる。

【0016】さらに、上述のデータ配信方法において、上記配信データが、上記出力手段としてのプリンタに、上記製作物としてのプリント物を出力させるためのデータとしてもよい。上記構成によれば、印刷データ配信システムを実現できる。

【0017】さらに、より不正利用の防止が求められる

場合には、上述のデータ配信方法において、上記復号工程は、出力許可を受けるサーバを認証する工程を含み、正規のサーバから出力許可を受け取った場合にのみ復号する方が望ましい。

【0018】上記の構成においては、サーバを認証する工程を含んでいるので、サーバになりすますためのコンピュータを利用者の端末に接続し、サーバになりかわって復号を許可するという、利用者の不正利用を防止することができる。

【0019】さらに、より不正利用の防止が求められる場合には、上述のデータ配信方法において、さらに上記サーバが、上記端末にパスワードを送信する工程と、上記端末が、上記パスワードに応じて上記サーバにパスワード要求を送信する工程と、上記サーバが、送信したパスワードと受信したパスワード要求とを比較して正規の端末であるか否かについて上記端末を認証する工程とを含み、認証に失敗した場合には、上記出力許可を上記端末に送信しないことが望ましい。

【0020】上記の構成によれば、サーバは、端末の認証が成功した場合にのみ処理を続けるので、処理を継続する場合の端末は、認証が成功した正規の端末であることが保証される。

【0021】また、サーバは、端末の認証に失敗した場合には出力許可を端末に送信しない。したがって、端末における潜在的な不正利用の可能性を減らすことができる。

【0022】さらに、上述のデータ配信方法において、上記配信工程の前に、上記配信データの配信される端末が上記消去工程を行う端末か否かを、上記サーバが確認する確認工程を含み、上記サーバは、確認できた場合にのみ、配信データを配信する方が好ましい。

【0023】上記の構成によれば、サーバは、端末が消去工程を行う端末である場合にのみ、配信データを配信する。したがってサーバより配信データを配信する端末は、出力後に配信データを消去するという適正な消去工程を行う端末であることが保証される。したがって、出力後の不正利用を防ぐことができる。

【0024】また、確認できなかった場合は配信しないので、データ配信における無駄なデータ流量を減らすことができるとともに、不正な配信データの流出のおそれを防ぐことができる。

【0025】さらに、より不正利用の防止が求められる場合には、上述のデータ配信方法において、さらに上記サーバが上記端末に第1のパスワードを送信し、上記端末が上記サーバに第1のパスワードに応じたパスワード要求を送信する、パスワード交換工程と、上記サーバが、送信した第1のパスワードと受信したパスワード要求とを比較して正規の端末であるか否かについて上記端末を認証する、端末認証工程と、認証が成功した場合に、上記サーバが、上記端末に上記出力許可として受信

10

20

30

40

50

したパスワード要求に応じた第2のパスワードを送信する、再送信工程と、上記端末が、送信したパスワード要求と受信した第2のパスワードとを比較して正規のサーバであるか否かについて上記サーバを認証する、サーバ認証工程とを含むことが望ましい。

【0026】上記の構成によれば、上記の端末認証工程およびサーバ認証工程において、それぞれサーバが端末を認証し、端末がサーバを認証するので、サーバと端末は相互に認証しあうことになり、データ配信におけるデータの流通の安全性を確保できる。

【0027】また、上記のように、パスワード交換工程における端末のパスワード要求送信は、サーバによる端末の認証のための返信であるとともに、端末によるサーバの認証のための送信でもあるので、兼用して配信におけるデータ流量を減らすことができる。

【0028】本発明に係る端末は、上記課題を解決するために、出力手段によって製作物を製作するための暗号化された配信データを記録する記録手段と、配信データの配信をサーバに要求し、上記記録手段に格納する配信要求手段と、上記サーバと通信して出力許可を受け取った場合にのみ記録手段に格納された配信データを復号する復号手段と、復号された配信データに応じた製作物を、上記出力手段に出力させる出力指示手段と、上記出力手段が製作物を出力した後、上記記録手段から配信データを消去する消去手段とを備えていることを特徴としている。

【0029】上記構成において、端末の配信要求手段は、配信データの配信要求を行い、配信された配信データを、記録手段に記録する。さらに、出力指示手段は、配信データを、出力手段に出力させると共に、消去手段

が出力後に記録手段から配信データを消去する。

【0030】上記構成では、端末は、出力後に記録手段から配信データを消去するので、上述の配信データの配信方法と同様に、配信データの不正利用を防止できると共に、利用者の手間をかけることなく、記録容量を削減でき、消去ミスを防止できる。

【0031】なお、上記記録手段は、たとえば、コンピュータ読み書き可能な記録媒体であって、端末に外付けされるものや、内蔵されるもの、および、分離して持ち歩き可能なものなどによって実現される。

【0032】本発明に係るサーバは、上記課題を解決するために、端末に接続された出力手段によって製作物を製作するための配信データを格納する配信データ保存手段と、暗号化された配信データの出力許可を上記端末へ送信する出力許可手段と、上記出力許可に応じて上記出力手段が製造物を出力した後で自らの配信データを消去する消去手段が設けられている端末から、配信要求を受けた場合、当該端末に暗号化した配信データを送信する配信手段とを備えていることを特徴としている。

【0033】上記構成において、サーバの配信手段は、

消去手段が設けられている端末から、配信要求を受信すると、上記端末へ暗号化された配信データを送信して、端末の記録手段に暗号化された配信データを格納させる。また、サーバの出力許可手段は、端末へ上記配信データの出力許可を送信する。一方、上記出力許可に応じて上記出力手段が製造物を出力した後で、端末の消去手段は、端末の記録手段から配信データを消去する。したがって、当該端末と組み合わせることで、上述のデータ配信方法と同様に、配信データを受信した端末側での不正利用を防止可能なデータ配信システムを実現できる。

【0034】さらに、上述のサーバには、上記端末にパスワードを送信し、その後に上記端末が上記パスワードに応じて上記サーバに送信するパスワード要求を受信し、それとともに、送信したパスワードと受信したパスワード要求とを比較して正規の端末であるか否かについて上記端末を認証し、認証に失敗した場合には上記出力許可を上記端末へ送信しない認証手段が備えられていることが望ましい。

【0035】上記構成において、サーバの認証手段は、端末にパスワードを送信し、端末がパスワードに応じてサーバに送信するパスワード要求を受信し、送信したパスワードと受信したパスワード要求とを比較して正規の端末であるか否かについて端末を認証し、認証に失敗した場合には暗号化された配信データを復号する出力許可を端末へ送信しない。したがって、端末における潜在的な不正利用の可能性を減らすことができる。

【0036】さらに上述のサーバには、上記端末から配信要求を受けた場合に、当該端末が、上記消去手段を備えているか否かを確認し、確認できた場合にのみ、上記配信手段に配信させる確認手段が設けられていてもよい。

【0037】上記の構成によれば、まず端末に上記消去手段が備えられているか否か確認を行い、確認できた場合にのみ、配信データを配信する。したがって、サーバより配信データを配信する端末に、適正な消去手段が備えられていることが保証される。したがって、出力後の不正利用を防ぐことができる。

【0038】さらに、上述のサーバは、上記確認手段によって、上記端末が消去手段を備えていないと判断された場合、上記端末を上記消去手段として動作させるためのプログラムまたはデータを、上記端末に送信する送信手段を備えていてもよい。上記動作させるためのデータとして、例えば上記動作させるためのプログラムをダウンロードすることのできるURL (Uniform Resource Locator) がある。

【0039】上記の構成によれば、消去手段が端末に備えられていない場合には、上記端末を上記消去手段として動作させるためのプログラムまたはデータを送信するので、簡単に上記端末を上記消去手段としても動作させることができるようになり、利用者にとって便利であ

10

20

30

40

50

る。また、利用者に、上記端末に上記消去手段を備えるようにうながすことができるので、配信事業者にとっても、便利である。

【0040】上記の構成によれば、サーバより配信データを配信する端末には、出力後に配信データを消去するという適正な消去手段が備えられていることが保証される。したがって、出力後の不正利用を防ぐことができる。

【0041】さらに、上述のサーバには、上記配信手段が配信する配信データを、可変の暗号キーで暗号化する暗号化手段と、上記配信手段が配信する配信データの復号キーを示すデータを配信先の上記端末へ通知する復号キー通知手段とが設けられていてもよい。上記の構成によれば、複数の暗号化パターンを用いることにより、セキュリティのレベルが高まるので、安心して用いることができる。

【0042】さらに、上述のサーバは、上記端末への配信データの配信に応じて課金処理する課金手段を備えていてもよい。上記の構成によれば、システムを有料として、課金処理を行なうことができ、配信事業者にとって便利である。なお、上記の課金処理手段は、例えば、事前のユーザ登録、クレジットカードの番号送付、電子マネーなどによって実現される。

【0043】また、本発明に係る、データ配信システムは、上記課題を解決するために、上記端末に接続された出力手段によって製作物を製作するための配信データを格納する配信データ保存手段、上記出力許可を上記端末へ送信する出力許可手段、および、上記端末から配信要求を受けた場合、当該端末に暗号化した配信データを送信する配信手段が設けられているサーバと、上述の端末とを含んでいることを特徴としている。

【0044】上記の構成によれば、端末やサーバが、それぞれ上記のように、動作し、機能する。したがって、配信データの不正利用を防止できると共に、利用者の手間をかけることなく、端末に必要な記録容量を削減でき、消去ミスを防止可能なデータ配信システムを実現できる。

【0045】また、本発明に係るプログラムは、記録手段を備えるコンピュータで実行するためのプログラムであって、上記課題を解決するために、サーバと通信して、出力手段によって製作物を製作するための配信データの出力許可を受け取った場合にのみ、上記記録手段に格納され、暗号化されている配信データを復号し、上記出力手段に出力させる出力指示手段、並びに、上記出力手段が製作物を出力した後、上記記録手段から配信データを消去する消去手段として、上記コンピュータを実行させることを特徴としている。上記プログラムがコンピュータで実行されると、コンピュータは、上述の復号、出力、消去工程を実施する端末として動作する。

【0046】したがって、上述の配信データの配信方法

と同様に、不正利用を防止できると共に、利用者の手間をかけることなく、記録容量を削減でき、消去ミスを防止できる。

【0047】また、本発明に係る記録媒体は、上記課題を解決するために、上述のプログラムを記録した、コンピュータ読取り可能な記録媒体である。上記記録媒体が、コンピュータで読み取られ、プログラムがコンピュータで実行されると、コンピュータは、上述の端末として動作する。したがって、上記端末と同様に、配信データの不正利用を防止できると共に、利用者の手間をかけることなく、記録容量を削減でき、消去ミスを防止できる。

【0048】また、本発明に係るプログラムは、上記課題を解決するために、上述のサーバの各手段としてコンピュータを動作させるための、プログラムである。上記プログラムがコンピュータで実行されると、コンピュータは、上述のサーバとして動作する。したがって、上記サーバと同様に、不正利用を防止できると共に、利用者の手間をかけることなく、記録容量を削減でき、消去ミスを防止できる。

【0049】また、本発明に係る記録媒体は、上記課題を解決するために、上述のプログラムを記録した、コンピュータ読取り可能な記録媒体である。上記記録媒体が、コンピュータで読み取られ、プログラムがコンピュータで実行されると、コンピュータは、上述のサーバとして動作する。したがって、上記サーバと同様に、不正利用を防止できると共に、利用者の手間をかけることなく、記録容量を削減でき、消去ミスを防止できる。

【0050】

【発明の実施の形態】本発明の一実施形態について、図を参照して説明する。まず、図2として、本実施形態の印刷データ配信システム1の全体構成を示す。印刷データ配信システム1は、利用者の用いる端末2と、配信事業者側のサーバ3とを含んでおり、端末2はプリンタ4に接続されている。さらに、端末2は、インターネット等の通信回線5を介して、配信事業者側のサーバ3に接続されている。

【0051】次に、図3として配信事業者側のサーバ3の構成を示す。サーバ3には、印刷データ保存領域（配信データ保存手段）6と、課金処理部（課金手段）7と、暗号化処理部8と、パスワード処理部9とが、備えられている。ここで、暗号化処理部8が、特許請求の範囲に記載の配信手段および認証手段に対応する。また、パスワード処理部9が、特許請求の範囲に記載の認証手段に対応する。

【0052】印刷データ保存領域6には、配信するための印刷データが保存される。課金処理部7は、印刷データの配信に伴って、課金処理する。暗号化処理部8は、端末2からの印刷データ配信要求を受信し、それに応じて、予め定められた暗号キーで印刷データの暗号化を行

い、暗号化した印刷データを送信する。

【0053】パスワード処理部9には、端末2からの印刷データ配信要求の際等に、印刷データにパスワードを付加して端末2へ送信させる、パスワード作成処理部10と、端末2から復号許可（出力許可）要求としてのパスワード要求を受信するとともに、復号許可および自らの認証のために、端末2へパスワードを送信する、パスワード送受信処理部11（出力許可手段）とが備えられている。

【0054】そして、図4として、利用者側の端末2の構成を示す。端末2には、配信された印刷データを一時的に記録しておくための印刷データ保存領域（記録手段）12と、印刷プログラムによって実現されるプリンタドライバ13と、サーバ3へ配信要求を行い、送信される印刷データを受信するダウンロード部（配信要求手段）14とが備えられていて、さらに、プリンタドライバ13には、復号処理部（復号手段）15、印刷処理部16、および、パスワード処理部17が備えられている。上記のダウンロード部14は、例えばWebブラウザなどで実現される。

【0055】ダウンロード部14は、上記サーバ3へ、印刷データの配信要求を行い、配信された印刷データを、印刷データ保存領域12へと一時的に記録する。また、復号処理部15は、暗号化された印刷データを復号する。

【0056】印刷処理部16には、印刷実行処理部（出力指示手段）18、印刷データ認識処理部19、および、印刷データ削除処理部（消去手段）20が備えられている。印刷実行処理部18は、復号された印刷データをプリンタ用のデータへと変換し、得られたプリンタ用のデータを図2に示すプリンタ4へ送信して、印刷させる。印刷データ認識処理部19は、印刷データ保存領域12に一時的に記録されている印刷データを認識する。印刷データ削除処理部20は、上記印刷実行処理部18によって印刷が実行された後で、印刷データ保存領域12に一時的に記録されていた印刷データ、および、プリンタ用のデータを、削除する。

【0057】パスワード処理部17には、パスワード送受信処理部21とパスワード照合処理部22とが備えられている。パスワード送受信処理部21は、復号許可のパスワードを上記サーバ3へ要求し、そして、サーバ3が復号を許可した場合に、サーバ3からそのパスワードを受信する。パスワード照合処理部22は、印刷データに付加されたパスワードと、復号許可のパスワードとを照合する。

【0058】以上の構成をもつ本実施形態における、印刷データ配信における動作を、図1のフローチャートを用いて説明する。図1において、右側の手順は配信事業者側のサーバ3における手順を示し、左側の手順は利用者側の端末2における手順を示す。

【0059】始めに、ステップS1として、利用者側の端末2のダウンロード部14が、サーバ3に対して、印刷データの配信を要求する。次にステップS2で、サーバ3の暗号化処理部8が、端末2からの配信要求を受信する。

【0060】ステップS3において、課金処理部7が課金処理する。課金処理では、配信要求された印刷データの料金を、利用者から徴収する。利用者を特定するため、例えば、前もってユーザ登録を行なっており、クレジットカードの番号を送信させたりすることで、徴収することができる。また、電子キャッシュを発行しておくことによっても、徴収することができる。

【0061】ステップS4において、サーバ3の暗号化処理部8が、印刷データを暗号化する。ステップS5においては、パスワード作成処理部10が、印刷データに対するユニークなパスワードを作成する。ステップS6では、パスワード作成処理部10が、印刷データにパスワードを付加する。ステップS7において、サーバ3の暗号化処理部8は、パスワードが付加された印刷データを、端末2のダウンロード部14へと送信する。

【0062】ステップS8では、端末2のダウンロード部14が、受信した印刷データを、印刷データ保存領域12に保存し、さらに、印刷データ認識処理部19が、印刷データ保存領域12に一時保存された印刷データを認識する。また、端末2のパスワード送受信処理部21は、印刷データに付加されていたパスワードを受信する。

【0063】ステップS9で、端末2のパスワード送受信処理部21は、サーバ3のパスワード送受信処理部11へ、復号許可（出力許可）の要求としてステップS8で受信したパスワードと同一のパスワード要求など、当該パスワードに応じたパスワード要求を送信する。このパスワード要求送信は、サーバ3による端末2の認証のための返信であるとともに、端末2によるサーバ3の認証のための送信でもある。ステップS10で、サーバ3のパスワード送受信処理部11が、パスワード要求を受信する。そして、ステップS11において、パスワード作成処理部10は、送信したパスワードと受信したパスワード要求を比較し、端末2の認証に成功すると、印刷データを配信した時と同じパスワードを作成し、そして、パスワード送受信処理部11は、作成されたパスワードを、端末2のパスワード送受信処理部21へ、復号許可として送信する。

【0064】一方、上記ステップS11において、サーバ3のパスワード作成処理部10が、端末2の認証に失敗すると、サーバ3は復号許可を出せないと判断する。この場合、パスワード送受信処理部11は、パスワード作成処理部10によって作成される、印刷データ配信時とは異なるパスワードを送信する。

【0065】ステップS12では、端末2のパスワード

送受信処理部21がパスワードを受信する。ステップS13では、パスワード送受信処理部21で受信したパスワードを、パスワード照合処理部22が、端末2の図示しないメモリ上に一時保存し、受信したパスワードと印刷データに付加されていたパスワードとを照合する。照合した結果、パスワードが一致すれば、パスワード照合処理部22は、認証が成功し、正規のサーバ3から復号許可が得られたものと判断し、復号処理部15に、印刷データを復号させる。これとは逆に、一致しない場合には、認証が不成功で、正規のサーバ3からは復号許可が得られなかったものとして、復号処理部15に復号させないので、処理が終了する。

【0066】上記ステップS13で、パスワードの照合に成功し、正規のサーバ3からの復号許可が確認されると、ステップS14では、復号処理部15が、印刷データ保存領域12に保存されていた印刷データの読み込みを行う。

【0067】次にステップS15では、復号処理部15が、暗号化された印刷データを復号する。ステップS16で、印刷実行処理部18は、復号された印刷データを、プリンタ用のデータへと変換する。ステップS17においては、印刷実行処理部18が、プリンタ用のデータを、プリンタ4に送信し、印刷させる。上記ステップS17で、印刷が終了すると、ステップS18では、印刷データ削除処理部20が、印刷データ保存領域12にある印刷データ、メモリ上に一時保存されたパスワード、復号された印刷データ、および、プリンタ用のデータを削除する。

【0068】上記の構成において、印刷データの印刷に失敗し、印刷が中断された場合には、プリンタ用データは消去されるが、印刷データの消去は行なわれない。したがって、印刷が中断された場合でも、暗号化された印刷データは端末2に残り、端末2は、再度印刷を試みることができる。

【0069】本実施形態における、端末2およびサーバ3の動作は、特許請求の範囲に記載の、配信工程、復号工程、出力工程、消去工程を順次実行するものである。すなわち、ステップS7でサーバ3が印刷データを送信し、ステップS8において端末2が印刷データを受信し格納することが、配信工程に相当する。ステップS12で復号許可としてのパスワードを受信し、ステップS13でパスワードを照合し、ステップS15で暗号化された印刷データを復号することが、復号工程に相当する。ステップS16でプリンタ用データに変換し、ステップS17でプリンタに送信し印刷させるまでが、出力工程に相当する。ステップS18で消去するのが、消去工程に相当する。

【0070】本実施形態の印刷データ配信システム1では、以上のように、印刷が終了すると、復号された印刷データおよび印刷データ自体は、ステップS18で削除

される。したがって、印刷後における、復号された印刷データおよび印刷データ自体の不正な複製および利用を防ぐことができる。

【0071】また、ステップS18で復号された印刷データおよび印刷データ自体は削除されるので、印刷物が残るため不要となる復号された印刷データおよび印刷データ自体は、印刷後には消去される。したがって、利用者にとって無駄な記録容量を使わずに済む。また、利用者自身による消去の作業は不要になるので、利用者にとって印刷処理が簡単となる。

【0072】また、本実施形態では、上記ステップS7でサーバ3より送信される印刷データが暗号化されているので、復号許可を受けた端末2がプリンタ4に印刷させるまで中身を見ることはできない。また、復号せずに印刷したとしても、意味のない印刷物しか得ることができない。したがって、複製することによる不正利用を防ぐことができる。

【0073】さらに、上記の方法においては、ステップS17で印刷した後、ステップS18で印刷データを消去するので、印刷データは必ず印刷を行なった後に消去される。したがって、間違って印刷前に印刷データを消去するということは、おこらない。

【0074】さらに、本実施形態のシステムにおいては、サーバ3に、課金処理する課金処理部7が備えられている。上記の構成によれば、システムを有料として、課金処理できるので、配信事業者にとって便利である。

【0075】また、本実施形態のシステムにおいては、端末2のダウンロード部14が、配信要求を行い、印刷データを受信するという構成である。ダウンロード部14としては、コンピュータに備えられているWebブラウザや、ftpプログラムなどを用いることができるので、新たな構成を付け加えることなく、印刷データを要求、受信することができる。上記のダウンロード部14を、プリンタドライバ13の一部として実現することも可能である。その場合には、ひとまとまりのプログラムであるプリンタドライバ13のみで、印刷データの要求、受信ができるので、利用者にとって便利である。

【0076】また、上記ステップS9で、端末2がサーバ3へパスワードを要求し、ステップS12でサーバ3から送信されるパスワードを受信して、サーバ3を認証し、復号許可を得るので、サーバ3になりすますためのコンピュータを利用者の端末2に接続し、サーバ3になりかわって復号を許可するという、利用者の不正利用を防止することができる。

【0077】さらに、上記の方法においては、上記ステップS7でサーバ3が端末2に印刷データとともにパスワードを送信し、ステップS9で端末2がサーバ3に上記パスワードに応じたパスワード要求を送信し、ステップS11でサーバ3が送信したパスワードと受信したパスワード要求とを比較して正規の端末であるか否かにつ

いて端末2を認証し、サーバ3は端末2の認証が成功した場合にのみ復号許可としてのパスワードを送信するので、ステップS13においてパスワードの照合が成功する場合の端末2は、認証が成功した正規の端末であることが保証される。また、サーバ3は、端末2の認証に失敗した場合には復号許可としての正規のパスワードを端末2に送信しないので、端末2における潜在的な不正利用の可能性を減らすことができる。

【0078】また、上記の方法においては、ステップS9で端末2がサーバ3にパスワード要求を送信し、ステップS11で上記サーバ3による端末2の認証が成功した場合にはサーバ3はパスワードを作成し復号許可として端末2に送信し、ステップS12で復号許可を受信することによって端末2がサーバ3を認証する。したがって、ステップS7からステップS12までのパスワードのやりとりによって、サーバ3と端末2は相互に認証しあうことになり、データ配信におけるデータの流通の安全性を確保できる。また、上記のように、端末2のパスワード要求送信は、サーバ3による端末2の認証のための返信であるとともに、端末2によるサーバ3の認証のための送信でもあるので、兼用して配信におけるデータ流量を減らすことができる。

【0079】本実施形態では、上記のように、ステップS7でサーバ3から端末2にパスワードを送信し、ステップS9で端末2がサーバ3に上記パスワードに応じてパスワード要求を送信し、ステップS11でサーバ3において送信したパスワードと受信したパスワード要求を比較することによって端末2が正規の端末であることが認証され、認証が成功した場合にのみサーバ3は端末2に復号許可としてのパスワードを送信する。そして、正規のサーバ3から復号許可を得た場合にのみ、ステップS16ないしステップS17において、印刷データが復号、印刷され、印刷終了後にステップS18において印刷データが消去されるので、端末2は、許可された印刷データのみを印刷し、消去できる。つまり、端末2は、サーバ3から印刷を許可された時にのみ、その印刷データを一度だけ印刷することができる。したがって、印刷データの複製による不正利用を防ぐことができる。また、利用者に、解読を試みさせないことによって、潜在的な不正利用の危険を防止することができる。

【0080】また、上述のように、サーバ3の暗号化処理部8は、暗号化したデータを端末2に送信するので、受信した端末2側での印刷データの不正利用を防ぐことができる。また、端末2側において、印刷データや印刷プログラムの不正な複製が行なわれたとしても、サーバ3側で認証を行ない、成功した場合のみ復号許可を送信するので、不正な複数回利用を防ぐことができる。

【0081】なお、上記第1あるいは後述の各実施形態において、端末2・サーバ3などを構成する各部材は、CPUなどの演算手段が、ROMやRAMなどの記録媒

体に格納されたプログラムを実行することで実現される機能ブロックであってもよいし、同様の処理を行うハードウェアで実現してもよい。また、処理の一部を行うハードウェアと、当該ハードウェアの制御や残余の処理を行うプログラムを実行する上記演算手段とを組み合わせても実現することもできる。さらに、上記演算手段は、単体であってもよいし、装置内部のバスや種々の通信路を介して接続された複数の演算手段が共同してプログラムを実行してもよい。

【0082】上記プログラムは、プログラム自体や当該プログラムを作成するためのデータなどを示すプログラムデータを記録媒体に格納し、当該記録媒体を配付したり、あるいは、上記プログラムデータを、有線または無線の通信手段で送信したりして配付され、上記演算手段で実行される。

【0083】なお、上記の説明においては、ある機能を特定の処理部が実行して、請求項に記載の手段として働くものとして記載したが、本発明の本質はそれに限るものではなく、要するに各手段が全体として実行されるものであればよい。例えば、一つのサーバが印刷データ保存手段として機能し、そしてそれとは別のサーバがのこの配信手段などとして働き、それらが互いにネットワーク接続されているような構成でも構わない。また、プリンタへの接続は、端末から直接でなくても、間に何台かのコンピュータを介したネットワーク経由でもよい。

【0084】また、認証が不成功の場合、上記例では、復号許可ではないパスワードを送信し、端末側の照合が失敗するようになっているが、単に何も送信しないようにしてもよい。

【0085】また、上記においては、サーバ3が課金処理部7を有するものとして説明したが、サーバ3が課金処理部7をもたない構成も可能である。例えば、無料で割引券のための印刷データを配布するような場合には、課金処理部7は不要である。

【0086】印刷プログラムは、上記のようにプリンタドライバ13として実施すれば、復号処理部15、印刷実行処理部18、および、印刷データ削除処理部20が一体化され、プログラムの改ざんの可能性を減らすことができ、安全性が向上する。また、別の実施形態として、印刷プログラムは、プリンタの制御を行なったりはせず、印刷プログラムが、プリンタに付属のプリンタドライバを介して、プリンタに印刷させることもできる。この場合は汎用性が高まる。

【0087】さらに、別の実施形態として、暗号化のキーを固定せず、変化させる実施形態を説明する。本実施形態においては、図2におけるサーバ3および端末2に代わって、図5に示す構成のサーバ33および図6に示す構成の端末32が用いられている。

【0088】図5のブロック図に示すように、サーバ33には、図3の部材6～11と同様の、部材36～41

に加えて、暗号化キー作成処理部（暗号化手段、復号キー通知手段）54が備えられている。

【0089】暗号化キー作成処理部54は、まず、暗号化処理部38が暗号化において用いるキーを作成する。暗号化処理部38は、キーを用いて暗号化するのであるが、図3の構成においては、固定されたキーが用いられていた。それに対して、本実施形態においては、暗号化キー作成処理部54が、互いに異なるキーを作成し、暗号化処理部38がそれを用いて暗号化するので、内容が同じ印刷データであっても、暗号化された印刷データは、互いに異なる暗号化パターンになる。

【0090】さらに、暗号化キー作成処理部54は、復号のキーをパスワード処理部39に送信して、パスワードに付加させる。本実施形態のように、暗号化においてキーを変化させる場合には、復号のためのキーを端末32に伝える必要がある。ここでは、復号のためのキーを示すデータをパスワードに付加して端末32に送信することにより、端末32側での復号を可能としている。

【0091】また、図6のブロック図に示すように、端末32には、図4の部材12～22と同様の、部材42～52に加えて、復号キー受信部53が備えられている。復号キー受信部53は、パスワード送受信処理部51と交信し、パスワードに付加された復号のキーを受信する。

【0092】次に、上述のサーバ33、端末32を備えた構成のシステムにおける、データ配信の動作を説明する。この場合の動作は、暗号化キーが固定の図1の場合と比べて、ステップS5とステップS15とが異なっている。

【0093】すなわち、ステップS5においては、暗号化キー作成処理部54が、暗号化のキーを作成し、パスワード作成処理部40へ送信する。また、パスワード作成処理部40が、印刷データに対するユニークなパスワードを作成し、受信したキーをパスワードに付加する。

【0094】また、ステップS15では、上述のステップS13においてパスワード照合処理部52が図示しないメモリに格納していたパスワードから、復号キー受信部53が、付加されていた復号のキーを取り出し、復号処理部45へと送信する。そして、復号処理部45が、当該キーを用いて暗号化された印刷データを復号する。

【0095】上記の構成では、以上のように、サーバ33の暗号化キー作成処理部54が、暗号化処理部38の暗号化キーを変化させると共に、復号キーを示すデータを端末32に送信させている。また、端末32の復号キー受信部53が、サーバ33から指定された復号キーによって、復号処理部45に復号させている。したがって、内容が同じ印刷データであっても、サーバ33と端末32との間で伝送される印刷データは、複数の暗号化パターンとなる。この結果、セキュリティのレベルが高まるので、印刷データの著作権者は、より安心して、印

刷データの配信を許可できる。

【0096】次に、本発明のもう一つ別の実施形態として、サーバが、端末に印刷プログラムが備えられているか確認し、備えられていない場合には印刷データ配信を中止する場合を説明する。本実施形態においては、図2のサーバ3および端末2に代わって、図7のサーバ63および図8の端末62が用いられている。

【0097】まず、印刷プログラムが備えられている場合の構成について、図7および図8を用いて説明する。本実施の形態におけるサーバ63の構成は、図7のブロック図で示す通りである。サーバ63には、図3の部材6～11と同様の部材66～71に加えて、さらに、ドライバ確認中止処理部（確認手段）83が備えられている。ドライバ確認中止処理部83は、暗号化処理部68が端末62からの配信要求を受信すると、それに応じて、印刷データを印刷させるための印刷プログラムのファイル名を送信することにより、印刷プログラムが端末62に備えられているか確認し、印刷プログラムが備えられていない場合に、印刷データ配信の処理を中止する。

【0098】また、図8のブロック図で示すように、端末62には、図4の部材12～22と同様の部材72～82に加えて、さらに、警告処理部84とファイル確認処理部85とが備えられている。警告処理部84は、印刷プログラムが端末62に備えられておらず、印刷データ配信が中止される場合に、端末62に警告を表示する。ファイル確認処理部85は、サーバ63のドライバ確認中止処理部83より送信されるファイル名を受信して、問題のファイルを検索できる。このような機能は、例えばコンピュータのOSの一部で実現されているので、汎用のコンピュータ等、印刷プログラムが備えられていない端末であっても、何ら支障なく、指定されたファイルを検索したり警告したりできる。

【0099】次に、この場合の動作を、プリンタドライバ73が備えられている場合と、備えられていない場合とをまとめて、図9のフローチャートを用いて説明する。本実施形態においては、図1のフローチャートにおけるステップS2と、ステップS3との間に、図9に示す各ステップS20～S28が挿入されている。なお、他の部分は、上述の説明と同じなので、説明を省略する。

【0100】まず、ステップS2で、サーバ63の暗号化処理部68が、利用者側の端末62からの印刷要求を受信する。次に、ステップS20で、ドライバ確認中止処理部83は、端末62のファイル確認処理部85に対し、ファイル名を送信して、プリンタドライバ73が正常に動作するために必要なファイルを検索要求するなどして、印刷可能なプリンタドライバ73が使用されているかを確認する。

【0101】そして、ステップS21として、端末62

のファイル確認処理部85が、検索要求された該当ファイル名を受信する。そして、ステップS22で、ファイル確認処理部85が、該当ファイルが存在するかを検索する。ステップS23において、ファイル確認処理部85によって、該当ファイルが存在するか否かが判定される。

【0102】上記ステップS23において該当するファイルが存在した場合、ステップS25において、端末62のファイル確認処理部85が、サーバ63のドライバ確認中止処理部83に、適正である旨を通知する。そして、つぎのステップS28で、ドライバ確認中止処理部83が、適正である旨の通知を受信する。この場合には、サーバ63において、ステップS3の課金処理が実行され、以下、図1と同様の動作が実行される。

【0103】それに対して、上記ステップS23において適正なファイルが存在しないと判断された場合、ステップS24では、端末62のファイル確認処理部85が、適正でない旨の通知を送信する。また、ステップS29では、警告処理部84が、適正なファイルが存在しない旨の警告を端末62に表示する。

【0104】そして、ステップS24で送信された通知を、ステップS26において、サーバ63のドライバ確認中止処理部83が受信する。この場合、次のステップS27では、ドライバ確認中止処理部83によって、データ配信の処理が中止される。

【0105】本実施形態では、上述のように、ドライバ確認中止処理部83が、まず端末62にプリンタドライバ73が備えられているか確認するので、端末62にすでにプリンタドライバ73が備えられている場合に、無駄に送信することを防げる。

【0106】また、プリンタドライバ73が端末に備えられていない場合に、印刷データ配信の処理を中止するので、印刷データ配信を行なった端末62には、印刷後に印刷データを消去するという適正なプリンタドライバ73が備えられていることが保証される。したがって、印刷後の不正利用の可能性を減らすことができる。

【0107】また、備えられていることが確認できなかった場合は配信しないので、データ配信における無駄なデータ流量を減らすことができるとともに、不正な配信データの流出のおそれを防ぐことができる。

【0108】なお、上記の端末62には、指定されたファイル名のファイルを検索する、ファイル確認処理部85、および、警告を行なう警告処理部84が備えられている。コンピュータのOSの一部で上記の機能が実現されるので、それを利用すれば、あらたな構成を必要としない。

【0109】また、上記の構成においては、ドライバ確認中止処理部83が、端末62へファイル名を検索要求して、端末62に該当ファイルが存在しない場合には、警告処理部84に警告させる。したがって、利用者に適

正なプリンタドライバ73を備えるよう促すことができる。

【0110】そして、上記の実施形態においては、端末62の警告処理部84は、端末62に備えられているが、始めはサーバ63に備えられていて、その後に端末62に送信することもできる。または、警告のための信号を、サーバ63が送信するようにしてもよい。いずれの場合であっても、利用者に警告を与えることができれば、上記の効果をを得ることができる。

10 【0111】また、ファイル確認処理部85も、同様に、始めはサーバ63に備えられていて、端末62に送信するようにできる。また、上記の実施形態においては、プログラムが存在するかどうかの確認は、ファイル名を送信することによって行なわれているが、その他の手段を用いることもできる。例えば、検索すべきファイル名を既に保持したファイル確認の手段がサーバに備えられ、それを端末に送信するようにしてもよい。このような構成にすれば、端末62での、ファイル確認処理部を用いた、利用者による不正利用の虞れを削減できる。

20 【0112】また、上記実施形態においては、検索結果が適正でない場合には、適正でない旨をサーバ63に送信しているが、そうでなく、単に結果を送信せずにいて、サーバ63で印刷データ配信の処理を中止することもできる。その場合には、例えば、サーバ63側で、一定時間経過しても応答がない場合に処理を打ち切るようにする。また、適正でない場合の送信と、上記打ち切りとを併用することもできる。上記打ち切りを用いれば、サーバ63での、印刷データ配信の処理の負担を軽減することができる。

30 【0113】なお、警告処理において、適正なプリンタドライバ73が入手できるように、警告処理部84が、ネットワーク上にあるプリンタドライバ73のダウンロードサイトのアドレスを、警告と同時に表示することもできる。そうすれば、端末62に適正なプリンタドライバ73を備えさせることが容易になる。また、プリンタドライバ73をすぐに手に入れることができるので、利用者にとって便利である。

40 【0114】次に、本発明のもう一つ別の実施形態として、サーバが、端末に印刷プログラムが備えられているかどうか確認し、備えられていない場合に、印刷プログラムを送信する場合を説明する。本実施形態においては、図2におけるサーバ3および端末2に代わって、図10のサーバ93および図11の端末92が用いられる。

【0115】まず、印刷プログラムが備えられている場合の構成について、図10および図11を用いて説明する。本実施の形態におけるサーバ93の構成は、図10のブロック図で示す通りである。サーバ93には、図7の部材66〜71と同様の部材96〜101が備えられ、図7におけるドライバ確認中止処理部83の代わり

に、さらに、ドライバ確認処理部(確認手段)113と、プログラム送信部(送信手段)114とが備えられている。ドライバ確認処理部113は、暗号化処理部98が端末92からの配信要求を受信すると、それに応じて、印刷データを印刷させるための印刷プログラムが端末92に備えられているか否かを、確認する。プログラム送信部114は、印刷プログラムが端末92に備えられていない場合に、図示されない記憶部から、印刷プログラムを読み出して、端末92へ送信する。

【0116】また、図11のブロック図で示すように、10 端末92は、図8の警告処理部84を取り除いた構成であり、図8の部材72〜82、85と同様の部材102〜112、115が備えられている。

【0117】次に、この場合の動作を、プリンタドライバ103が備えられている場合と、備えられていない場合とをまとめて、図12のフローチャートを用いて説明する。本実施形態においては、図1のフローチャートにおけるステップS2と、ステップS3との間に、図12に示す各ステップS30〜S43が挿入されている。なお、他の部分は、上述の説明と同じなので、説明を省略20 する。

【0118】まず、ステップS2では、サーバ93の暗号化処理部98が、利用者側の端末92からの印刷要求を受信する。次に、ステップS30で、ドライバ確認処理部113は、端末92のファイル確認処理部115に対し、ファイル名を送信して、プリンタドライバ103が正常に動作するために必要なファイルを検索要求するなどして、印刷可能なプリンタドライバ103が使用されているかを確認する。

【0119】そして、ステップS31では、端末92の30 ファイル確認処理部115が、検索要求された該当ファイル名を受信する。そして、ステップS32で、ファイル確認処理部115が、該当ファイルが存在するか否かを検索する。ステップS33において、ファイル確認処理部115が、該当ファイルが存在するか判定する。

【0120】ステップS33において該当するファイルが存在した場合、ステップS35では、ファイル確認処理部115が、サーバ93のドライバ確認処理部113に、適正である旨を通知する。そして、つぎのステップS43で、サーバ93のドライバ確認処理部113が、40 適正である旨の通知を受信する。この場合には、サーバ93において、ステップS3の課金処理が実行され、以下、図1と同様の動作が実行される。

【0121】それに対して、ステップS33において適正なファイルが存在しないと判断した場合の、ステップS34では、端末92のファイル確認処理部115が、適正でない旨の通知を送信する。

【0122】この場合、ステップS36において、ステップS34における通知を、サーバ93のドライバ確認処理部113が受信する。ステップS37では、プログ50

ラム送信部114によって、端末92へプリンタドライバ103が送信される。

【0123】ステップS38では、端末92がプリンタドライバ103を受信する。ステップS39でプリンタドライバ103がインストールされると、ステップS40において、ファイル確認処理部115が、再びファイル名を検索する。この場合は該当するファイルが存在するので、ステップS41において、ファイル確認処理部115が、サーバ93のドライバ確認処理部113に、適正である旨を通知する。そして、次のステップS42で、サーバ93のドライバ確認処理部113が、適正である旨の通知を受信する。次にステップS3で課金処理が行なわれ、以下、図1と同様の動作が実行される。

【0124】本実施形態では、上述のように、ドライバ確認処理部113が、まず端末92にプリンタドライバ103が備えられているか否かを確認するので、端末92にすでにプリンタドライバ103が備えられている場合に、無駄に送信することを防げる。

【0125】また、ドライバ確認処理部113が、プリンタドライバ103が端末に備えられているかどうか確認し、プリンタドライバ103が端末に備えられていない場合には、プログラム送信部114が、プリンタドライバ103を送信し、その後印刷データを配信するので、印刷データ配信を行なった端末92には、印刷後に印刷データを消去するという適正なプリンタドライバ103が備えられていることが保証される。したがって、印刷後の不正利用の可能性を減らすことができる。

【0126】なお、本実施形態においても、端末92に、図8に示す警告処理部84と同様の手段を備えさせて、端末92にプリンタドライバ103が備えられていない場合に、警告することもできる。そうすれば、利用者に適正なプリンタドライバ103を備えるよう促すことができる。さらに、その際、送信するプリンタドライバ103のインストール方法を表示することもできる。そうすれば、インストールしやすくなるので、利用者にとって便利である。

【0127】上記の構成において、プリンタドライバ103が端末に備えられていない場合に、プリンタドライバ103とともに、さらにインストールプログラムも送信することができる。この場合は、利用者は簡単にインストールすることができるので好ましい。また、インストールプログラムを用いてインストールさせるので、不正なインストールを防ぐことができる。

【0128】

【発明の効果】本発明に係るデータ配信方法は、以上のように、端末に接続された出力手段によって製作物を製作するための暗号化された配信データを、サーバから上記端末に配信し、当該端末の記録手段に格納する配信工程と、上記端末が、上記サーバと通信して出力許可を受け取った場合にのみ暗号化された配信データを復号する

復号工程と、上記端末が、復号された配信データに基づいて、上記出力手段に製作物を出力させる出力工程と、上記出力工程の後、上記記録手段から配信データを消去する消去工程とを含んでいる構成である。

【0129】したがって、出力が終わるとともに、配信データは削除されるので、出力後における、配信データの不正な複製および利用を防ぐことができるという効果を奏する。また、利用者に不要となった配信データの消去をさせることなく、無駄な記録容量を削減できるという効果を奏する。さらに、出力許可を受け取った場合にのみ復号、出力、消去をするので、その配信データを1度だけ出力することができ、したがって、端末側で複製することによる不正利用を防ぐことができるという効果を奏する。また、上記消去工程において、配信データは出力後に消去されるので、配信データの複製物は端末に残らず、端末の利用者が当該配信データの不正利用を試みる虞れを防ぐことができるという効果を奏する。

【0130】本発明に係るデータ配信方法は、以上のように、さらに、上述のデータ配信方法において、上記配信データが、上記出力手段としてのプリンタに、上記製作物としてのプリント物を出力させるためのデータとする構成である。したがって、印刷データ配信システムを実現できるという効果を奏する。

【0131】本発明に係るデータ配信方法は、以上のように、上記構成に加えて、上記復号工程は、出力許可を受けるサーバを認証する工程を含み、正規のサーバから出力許可を受け取った場合にのみ復号する構成である。

【0132】したがって、サーバを認証する工程を含んでいるので、サーバになりすますためのコンピュータを利用者の端末に接続し、サーバになりかわって復号を許可するという、利用者の不正利用を防止することができるという効果を奏する。

【0133】本発明に係るデータ配信方法は、以上のように、上記構成に加えて、さらに上記サーバが、上記端末にパスワードを送信する工程と、その後、上記端末が、上記パスワードに応じて上記サーバにパスワード要求を送信する工程と、それとともに、上記サーバが、送信したパスワードと受信したパスワード要求とを比較して正規の端末であるか否かについて上記端末を認証する工程とを含み、認証に失敗した場合には、上記出力許可を上記端末に送信しない構成である。

【0134】したがって、サーバは、端末の認証が成功した場合にのみ処理を続けるので、処理を継続する場合の端末は、認証が成功した正規の端末であることが保証されるという効果を奏する。

【0135】本発明に係るデータ配信方法は、以上のように、上記構成に加えて、上記配信工程の前に、上記配信データの配信される端末が上記消去工程を行う端末か否かを、上記サーバが確認する確認工程を含み、上記サーバは、確認できた場合にのみ、配信データを配信する

構成である。

【0136】したがって、サーバより配信データを配信する端末は、出力後に記録手段から配信データを消去するという適正な消去工程を行う端末であることが保証されるので、出力後の不正利用を防ぐことができるという効果を奏する。

【0137】本発明に係るデータ配信方法は、以上のように、上記構成に加えて、さらに上記サーバが上記端末に第1のパスワードを送信し、上記端末が上記サーバに第1のパスワードに応じたパスワード要求を送信する、パスワード交換工程と、上記サーバが、送信した第1のパスワードと受信したパスワード要求とを比較して正規の端末であるか否かについて上記端末を認証する、端末認証工程と、認証が成功した場合に、上記サーバが、上記端末に上記出力許可として受信したパスワード要求に応じた第2のパスワードを送信する、再送信工程と、上記端末が、送信したパスワード要求と受信した第2のパスワードとを比較して正規のサーバであるか否かについて上記サーバを認証する、サーバ認証工程とを含んでいる構成である。

【0138】したがって、上記の端末認証工程およびサーバ認証工程において、それぞれサーバが端末を認証し、端末がサーバを認証するので、サーバと端末は相互に認証しあうことになり、データ配信におけるデータの流通の安全性を確保できるという効果を奏する。

【0139】本発明に係る端末は、以上のように、出力手段によって製作物を製作するための暗号化された配信データを記録する記録手段と、配信データの配信をサーバに要求し、上記記録手段に格納する配信要求手段と、上記サーバと通信して出力許可を受け取った場合にのみ記録手段に格納された配信データを復号する復号手段と、復号された配信データに応じた製作物を、上記出力手段に出力させる出力指示手段と、上記出力手段が製作物を出力した後、上記記録手段から配信データを消去する消去手段とを備えている構成である。

【0140】したがって、端末は、出力後に記録手段から配信データを消去するので、上述の配信データの配信方法と同様に不正利用を防止できると共に、利用者の手間をかけることなく、記録容量を削減できるという効果を奏する。

【0141】本発明に係るサーバは、以上のように、端末に接続された出力手段によって製作物を製作するための配信データを格納する配信データ保存手段と、暗号化された配信データの出力許可を上記端末へ送信する出力許可手段と、上記出力許可に応じて上記出力手段が製造物を出力した後で自らの配信データを消去する消去手段が設けられている端末から、配信要求を受けた場合、当該端末に暗号化した配信データを送信する配信手段とを備えている構成である。したがって、当該端末と組み合わせることで、受信した端末側での不正利用を防止可能

なデータ配信システムを実現できるという効果を奏する。

【0142】本発明に係るサーバは、以上のように、さらに、上記端末にパスワードを送信し、その後上記端末が上記パスワードに応じて上記サーバに送信するパスワード要求を受信し、それとともに、送信したパスワードと受信したパスワード要求とを比較して正規の端末であるか否かについて上記端末を認証し、認証に失敗した場合には暗号化された配信データを復号する出力許可を上記端末へ送信しない認証手段が備えられている構成である。

【0143】したがって、サーバの認証手段は、正規の端末であるか否かについて端末を認証し、認証に失敗した場合には出力許可を端末へ送信しないので、端末における潜在的な不正利用の可能性を減らすことができるという効果を奏する。

【0144】本発明に係るサーバは、以上のように、上記構成に加えて、上記端末から配信要求を受けた場合に、当該端末が、上記消去手段を備えているか否かを確認し、確認できた場合にのみ、上記配信手段に配信させる確認手段が設けられている構成である。

【0145】したがって、まず端末に上記消去手段が備えられているか否か確認を行い、確認できた場合にのみ、配信データを配信するので、サーバより配信データを配信する端末に、適正な消去手段が備えられていることが保証され、出力後の不正利用を防ぐことができるという効果を奏する。

【0146】本発明に係るサーバは、以上のように、上記構成に加えて、上記確認手段によって上記端末が消去手段を備えていないと判断された場合、上記端末を上記消去手段として動作させるためのプログラムまたはデータを上記端末に送信する送信手段を備えている構成である。

【0147】したがって、消去手段が端末に備えられていない場合には、上記端末を上記消去手段として動作させるためのプログラムまたはデータを送信するので、簡単に上記端末を上記消去手段としても動作させることができるようになり、利用者にとって便利であるという効果を奏する。

【0148】本発明に係るサーバは、以上のように、上記構成に加えて、上記配信手段が配信する配信データを、可変の暗号キーで暗号化する暗号化手段と、上記配信手段が配信する配信データの復号キーを示すデータを配信先の上記端末へ通知する復号キー通知手段とが設けられている構成である。したがって、複数の暗号化パターンを用いることにより、セキュリティのレベルが高まるので、安心して用いることができるという効果を奏する。

【0149】本発明に係るサーバは、以上のように、上記構成に加えて、上記端末への配信データの配信に応じ

て課金処理する課金手段を備えている構成である。上記の構成によれば、システムを有料として、課金処理を行なうことができ、配信事業者にとって便利であるという効果を奏する。

【0150】また、本発明に係る、データ配信システムは、上述のように、上記端末に接続された出力手段によって製作物を製作するための配信データを格納する配信データ保存手段、上記出力許可を上記端末へ送信する出力許可手段、および、上記端末から配信要求を受けた場合、当該端末に暗号化した配信データを送信する配信手段が設けられているサーバと、上述の端末とを含んでいる構成である。

【0151】したがって、端末やサーバが、それぞれ上記のように、動作し、機能する。したがって、不正利用を防止できると共に、利用者の手間をかけることなく、端末に必要な記録容量を削減でき、消去ミスを防止可能なデータ配信システムを実現できるという効果を奏する。

【0152】本発明に係るプログラムは、記録手段を備えるコンピュータで実行するためのプログラムであって、以上のように、サーバと通信して、出力手段によって製作物を製作するための配信データの出力許可を受け取った場合にのみ、上記記録手段に格納され、暗号化されている配信データを復号し、上記出力手段に出力させる出力指示手段、並びに、上記出力手段が製作物を出力した後、上記記録手段から配信データを消去する消去手段として、上記コンピュータを実行させる構成である。

【0153】したがって、上記プログラムがコンピュータで実行されると、コンピュータは、上述の復号、出力、消去工程を実施する端末として動作するので、上述の配信データの配信方法と同様に、不正利用を防止できると共に、利用者の手間をかけることなく、記録容量を削減でき、消去ミスを防止できるという効果を奏する。

【0154】本発明に係る記録媒体は、以上のように、上述のプログラムを記録した、コンピュータ読取り可能な記録媒体である。上記記録媒体が、コンピュータで読み取られ、プログラムがコンピュータで実行されると、コンピュータは、上述の端末として動作する。したがって、上記端末と同様に、不正利用を防止できると共に、利用者の手間をかけることなく、記録容量を削減でき、消去ミスを防止できるという効果を奏する。

【0155】本発明に係るプログラムは、以上のように、上述のサーバの各手段としてコンピュータを動作させるための、プログラムである。上記プログラムがコンピュータで実行されると、コンピュータは、上述のサーバとして動作する。したがって、上記サーバと同様に、不正利用を防止できると共に、利用者の手間をかけることなく、記録容量を削減でき、消去ミスを防止できるという効果を奏する。

【0156】本発明に係る記録媒体は、以上のように、

上述のプログラムを記録した、コンピュータ読取り可能な記録媒体である。上記記録媒体が、コンピュータで読み取られ、プログラムがコンピュータで実行されると、コンピュータは、上述のサーバとして動作する。したがって、上記サーバと同様に、不正利用を防止できると共に、利用者の手間をかけることなく、記録容量を削減でき、消去ミスを防止できるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の一実施形態を示すものであり、印刷データ配信システムにおける動作を説明するフローチャートである。

【図2】上記印刷データ配信システムの全体構成を示す説明図である。

【図3】上記印刷データ配信システムのサーバの要部構成を示すブロック図である。

【図4】上記印刷データ配信システムの端末の要部構成を示すブロック図である。

【図5】本発明の他の実施形態を示すものであり、上記印刷データ配信システムのサーバの要部構成を示すブロック図である。

【図6】上記印刷データ配信システムの端末の要部構成を示すブロック図である。

【図7】本発明のさらに他の実施形態を示すものであり、印刷データ配信システムのサーバの要部構成を示すブロック図である。

【図8】上記印刷データ配信システムの端末の要部構成を示すブロック図である。

【図9】上記印刷データ配信システムにおける動作を説明するフローチャートである。

【図10】本発明のまた別の実施形態を示すものであり、印刷データ配信システムのサーバの要部構成を示すブロック図である。

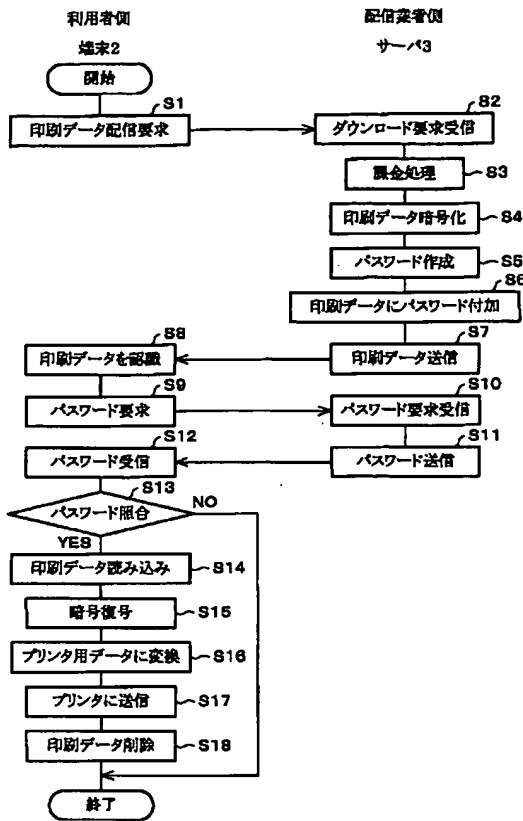
【図11】上記印刷データ配信システムの端末の要部構成を示すブロック図である。

【図12】上記印刷データ配信システムにおける動作を説明するフローチャートである。

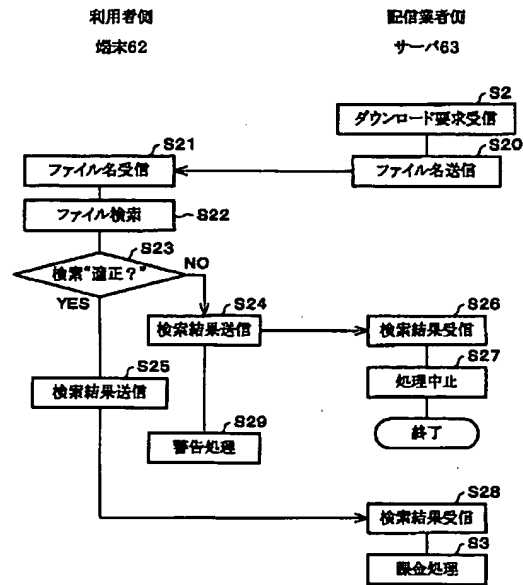
【符号の説明】

1	印刷データ配信システム	
2、32、62、92	端末	
3、33、63、93	サーバ	
4	プリンタ	
5	通信回線	
6、36、66、96	印刷データ保存領域（配信データ保存手段）	
7、37、67、97	課金処理部（課金手段）	
8、38、68、98	暗号化処理部（配信手段、認証手段）	
9、39、69、99	パスワード処理部（認証手段）	
11、41、71、101	パスワード送受信処理部（出力許可手段）	
12、42、72、102	印刷データ保存領域（記録手段）	
13、43、73、103	プリンタドライバ	
14、44、74、104	ダウンロード部（配信要求手段）	
15、45、75、105	復号処理部（復号手段）	
16、46、76、106	印刷処理部	
17、47、77、107	パスワード処理部	
18、48、78、108	印刷実行処理部（出力指示手段）	
19、49、79、109	印刷データ認識処理部	
20、50、80、110	印刷データ削除処理部（消去手段）	
53	復号キー受信部	
54	暗号化キー作成処理部（暗号化手段、復号キー通知手段）	
83	ドライバ確認中止処理部（確認手段）	
84	警告処理部	
85、115	ファイル確認処理部	
113	ドライバ確認処理部（確認手段）	
114	プログラム送信部（送信手段）	

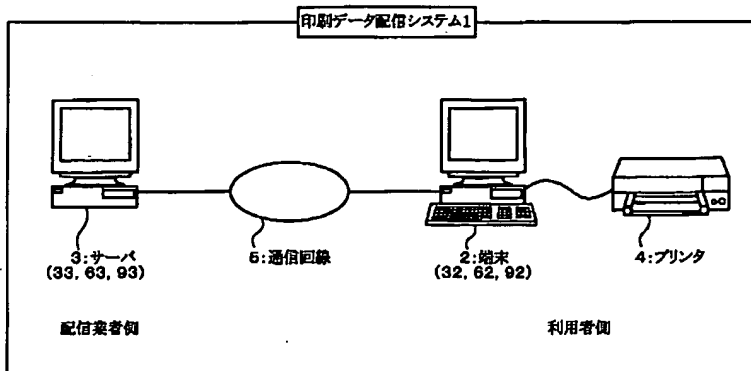
【図1】



【図9】



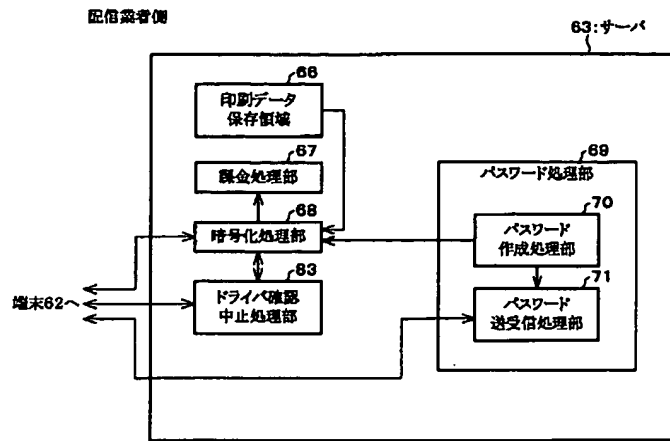
【図2】



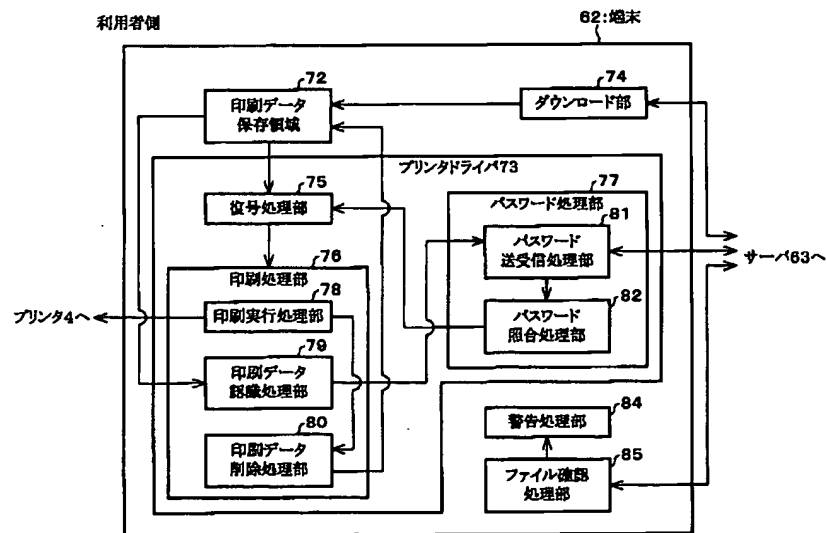


The diagram shows the internal components of the distribution system. On the left, a vertical line labeled "端末32へ" (to terminal 32) connects to a central processing unit. This unit contains several modules: at the top, a box labeled "印刷データ保存領域" (Print Data Storage Area) with reference numeral 36; below it, a box labeled "課金処理部" (Billing Processing Unit) with reference numeral 37; below that, a box labeled "暗号化処理部" (Encryption Processing Unit) with reference numeral 38; and at the bottom, a box labeled "暗号化キー作成処理部" (Encryption Key Creation Processing Unit) with reference numeral 54. Arrows indicate data flow: from the terminal connection point to the encryption processing unit (38), from the encryption key creation unit (54) to the encryption unit (38), from the encryption unit (38) to the billing unit (37), and from the encryption unit (38) to the password processing unit (39). The password processing unit (39) is a separate block containing three sub-units: "パスワード処理部" (Password Processing Unit) with reference numeral 39 at the top, "パスワード作成処理部" (Password Creation Processing Unit) with reference numeral 40 in the middle, and "パスワード送受信処理部" (Password Transmission/Reception Processing Unit) with reference numeral 41 at the bottom. An arrow points from the password creation unit (40) to the password transmission/reception unit (41).

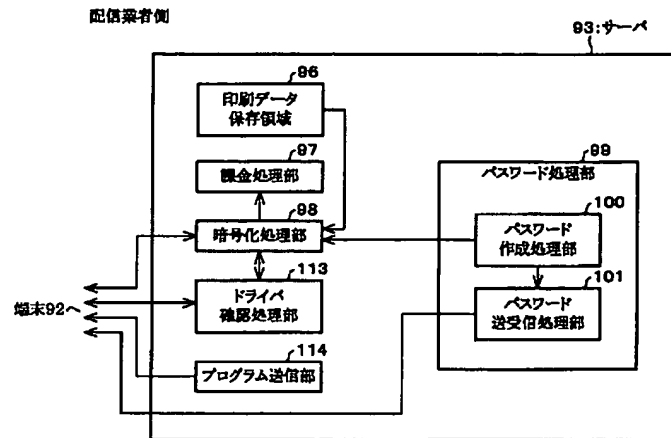
【図7】



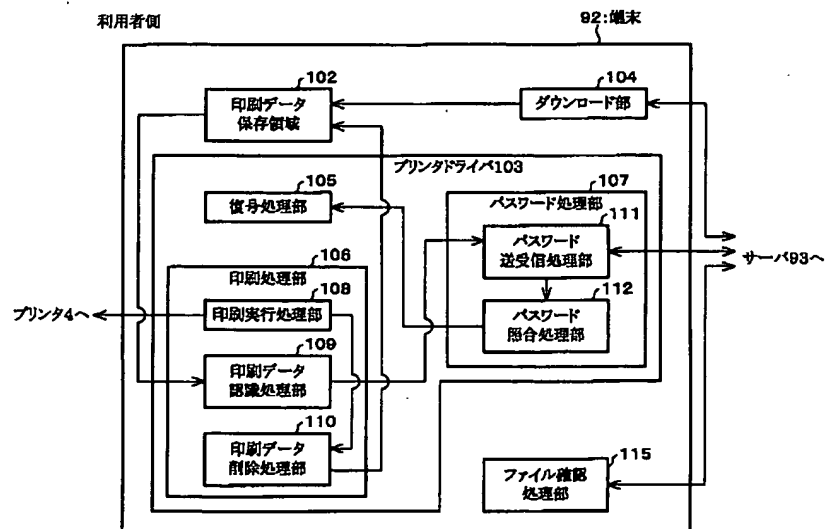
【図8】



【図10】



【図11】



【図12】

